REMARKS

Claims 1-15, 17-62, 64-80, and 82-88 are pending in this application, of which claims 29 and 76 are amended herein to correct typographical errors. All of the claims have been rejected. Claims 1-5, 10-15, 17-25, 28-62, 64-80, and 82-88 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Leporini et al. (US PG Pub. No. 2003/0182579) in view of Sprague et al. (US Pat. No 5,247,575), and claims 6-9, 26, and 27 have been rejected over the same combination in further view of Ozog et al. (US PG Pub. No. 2003/0033528). Reconsideration of claims 1-15, 17-62, 64-80, and 82-88 is respectfully requested.

As in the prior response, Applicants again note that the Sprague et al. reference, in the present Office action, is consistently misidentified with a publication number of an unrelated US Pre-Grant Publication to Okamoto et al. Likewise, the Examiner has continued to refer to outdated claim language in several instances rather than refer to the claim limitations as presently presented. The listing of claims, presented above, provides the claims as they presently stand. Appropriate correction is requested in any subsequent Office action.

Rejections Under 35 USC 103(a)

In paragraph 3 of the Office action, the Examiner rejected claims 1-5, 10-15, 17-25, 28-62, 64-80, and 82-88 under 35 U.S.C. §103(a) over Leporini et al. in view of Sprague et al. Claims 6-9, 26, and 27 were rejected over the same combination in further view of Ozog et al. in paragraph 39. Applicants transverse the rejection.

The Examiner alleges in the Office action that Leporini et al. teaches "a method for providing access control management to electronic data, the method comprising establishing a secured link with a client machine when an authentication request is received from the client machine, the authentication request including an identifier identifying a user of the client machine to access the electronic data, wherein the electronic data is secured in a format including security information and an encrypted data portion, the security information including file key and access rules and controlling

restrictive access to the encrypted data portion authenticating the user according to the identifier (see paragraphs 0003, 0004, 0008, 0015, 0024, 0027, 0036, 0041-0046, 005200203 [sic], 00437)." Applicants note that this does not reflect the current state of claim 1 as provided in the listing of claims, above.

The language of present claim 1 recites:

1. A method for providing access control management to electronic data, the method comprising:

establishing a secured link between a server providing the access control management and a client machine when an authentication request is received from the client machine, the authentication request including an identifier identifying a user of the client machine to access the electronic data, wherein the electronic data is not from the server but secured in a format including security information and an encrypted data portion, the security information including a file key and access rules and controlling restrictive access to the encrypted data portion;

authenticating the user according to the identifier; and

activating a user key after the user is authenticated, wherein the user key is used to access the access rules in the security information, the file key can be retrieved to decrypt the encrypted data portion only if access privilege of the user is successfully measured by the access rules.

Applicants first note, with respect to Leporini et al., that the Examiner has cited to upwards of 150 paragraphs but has not particularly indicated where the various limitations of claim 1 are to be found therein. It has apparently been left to the Applicants to discern how the cited reference supposedly reads on the claim. Accordingly, Applicants will provide an interpretation of Leporini et al. and invite the Examiner to either agree or offer an alternative interpretation with specific support therefore.

Applicants remind the Examiner that, per MPEP §706.07, "[t]he applicant who is seeking to define his or her invention in claims that will give him or her the patent protection to which he or she is justly entitled should receive the cooperation of the examiner to that end" and "[t]he examiner should never lose sight of the fact that in every case the applicant is entitled to a full and fair hearing, and that a clear issue between applicant and examiner should be developed, if possible, before appeal." Applicants seek the Examiner's cooperation and a full and fair hearing in order to define the claims, and believe that it is impossible to develop clear issues for appeal without an understanding of

how the Examiner aligns the teachings of the reference to the specific limitations of each claim.

Applicants also note 37 CFR §1.104(c) which provides that "[w]hen a reference is complex or shows or describes inventions other than that claimed by the applicant, the particular part relied on must be designated as nearly as practicable. The pertinence of each reference, if not apparent, must be clearly explained." Applicants assert that Leporini et al. is quite complex and describes inventions other than that claimed, and citing to over 15 continuous columns of the published application without further elaboration does not designate the particular parts relied on as nearly as possible. Greater specificity from the Examiner in future communications would be highly appreciated.

Independent claim 1 requires "establishing a secured link between a server providing the access control management and a client machine when an authentication request is received from the client machine." This requirement further necessitates the existence of "a client machine" and "a server providing the access control management." Moreover, the requirement necessitates a step of "establishing a secured link" between the server and the client machine "when an authentication request is received from the client machine."

Applicants propose that "a client machine" in Leporini et al. is the HDVR. While there are many components discussed in the reference that potentially could be considered a client machine, Leporini et al. specifically identifies the HDVR as a client in paragraph [0251], and Applicants view a hard disk video recorder as a machine. If the Examiner views some component other than the HDVR as the client machine, Applicants request that the Examiner explicitly identify the component and indicate the support in Leporini et al. for considering said component to be the client.

Applicants propose that "a server providing the access control management" is the CMPS server specifically referred to in paragraphs [0267], [0284], and [0330]. Here, too, there are a number of servers provided in Leporini et al., but Leporini et al. notes that "navigation and usage constraint information [is] associated with the CMPS server" (paragraph [0267]). The "navigation and usage constraint information" would appear to provide "access control management" in Leporini et al. Again, if the Examiner views a

different server as responsible for providing the access control management in Leporini et al., the Examiner is encouraged to explicitly provide and justify the alternative interpretation.

As noted above, the limitation of claim 1 being discussed requires "establishing a secured link" between the server and the client machine "when an authentication request is received from the client machine." Thus, claim 1 requires that the secured link is established when an authentication request is received from the client machine. Although Applicants note in Leporini et al. instances of secured links, connections, channels, and interfaces (e.g. [0296] [0309] [0317] [0329] [0347] [0355] [0360] [0364] [0380] [0404] [0410] [0423] [0436] [0437] [0439] [0443] [0444] and [0460]), none of these instances pertain to a link that is established between the HDVR and the CMPS server when the HDVR requests authentication.

For example, the references to secured connections found in paragraphs [0296], [0309], and [0317] do not involve the HDVR. These paragraphs pertain to the embodiments illustrated in FIGs. 24-26. In each instance, the secure connection is associated with either stage 407, 503, or 607. In each embodiment, the implicated stage is between the CMPS and the RCARD_device, and not the HDVR.

The references to secured connections identified in paragraphs [0329] - [0423] pertain to connections between SM CMPS and SM CAS (stage 1500 in FIG. 30, stages 1600 and 1612 in FIG. 32, and stage 1700 in FIG. 34). The communications between these two security modules (SM) take place within the decoder/receiver 13 (FIG. 2) and do not involve the HDVR (e.g. mass storage device 370 (FIG. 2). As evidence, Leporini et al. notes that "[t]he receiver/decoder itself comprises a daughter conditional access smartcard 48" (paragraph [0198], see FIG. 2) and "[t]he receiver/decoder portion of the CMPS 300 comprises a security module (in the form of a removable smartcard) 320 (not shown)" (paragraph [0199], see FIG. 2). The conditional access smartcard 48 is identified with the CAS SM in paragraph [0339].

Paragraph [0437] was particularly noted by the Examiner. This paragraph pertains to "APIs which may be included in the security library of the CMPS" and that are described in subsequent paragraphs, such as noted paragraphs [0439] – [0460]. These APIs "raise issues on the usage of a client-server model between the CMPS SM and the

group of equipment with which a secure connection (SAC) is established" (paragraph [0437]). Nowhere in these paragraphs is the HDVR implicated as a device with which the CMPS SM creates a secure connection.

Even if, *arguendo*, paragraphs [0437] – [0460] can be read to implicate that a secure connection is created between the CMPS SM and the HDVR, such a connection is to the CMPS SM (i.e. a smartcard) and not to the CMPS server identified above as the server of claim 1 that provides access control management. Moreover, there is no indication that such a secure connection is established "when an authentication request is received" from the HDVR.

Turning next to the requirement of claim 1 that "the authentication request include[s] an identifier identifying a user of the client machine to access the electronic data." Applicants note that Leporini et al. teaches that "[a]t the instigation of the HDVR sub-system, a session is opened with CMPS allowing the recovery of the CMM data at the time of each event" (paragraph [0265]) and "[a]t the time of arrival of this event, HDVR requests the CMM to obtain navigation and usage constraint information associated with the CMPS server" (paragraph [0267]). Although the HDVR makes a request, Applicants assert that the request does not constitute an authentication request because the request does not seek to authenticate. Rather, the request is for information, specifically navigation and usage constraint information. Even if, *arguendo*, it is assumed that a request for navigation and usage constraint information is a request for authentication, Applicants further note that Leporini et al. does not teach that the request includes an identifier identifying the user of the HDVR.

Claim 1 further requires "authenticating the user according to the identifier." Applicants recognize that, according to Leporini et al., "[i]n the personalisation mode the CMPS system is responsible for the creation of personalised copies by encrypting the CMM by a unique user key. This key moreover depends on a content identifier (content_id) serving to broaden the user key. All usage of recorded content requires a security module to be present to personalise the copy" (paragraph [0378]). As noted above, claim 1 requires that the identifier identify the user, yet in the personalization mode of Leporini et al., the unique "user" key depends on a content identifier. Thus, it actually identifies the content to the user, rather than actually identifying the user. Even

if the unique user key is viewed as an identifier that identifies the user, the user key is not used to authenticate the user in Leporini et al.

Lastly, claim 1 requires "activating a user key after the user is authenticated, wherein the user key is used to access the access rules in the security information, the file key can be retrieved to decrypt the encrypted data portion only if access privilege of the user is successfully measured by the access rules." The Examiner notes that Leporini et al. does not teach this limitation and alleges it can be found in Sprague et al. Applicants note that the Examiner asserted the same teaching for Sprague et al. in the prior Office action that followed the Appeal Brief, and Applicants replied in the response thereto with specific arguments as to why Sprague et al. does not disclose that "the *user key is used to access the access rules in the security information*, the file key can be retrieved *to decrypt the encrypted data portion* only if access privilege of the user is successfully measured by the access rules."

The Examiner, having found new grounds for rejection, has asserted that Applicants' arguments are moot and has avoided answering the substance of Applicants' arguments with respect to Sprague et al. Applicants therefore refer the Examiner to the arguments made in the previous response regarding the deficiencies of Sprague et al. For example, on page 6 of the prior response, Applicants pointed out that Sprague et al. does not disclose that "the ***user key is used to access the access rules in the security information***, the file key can be retrieved ***to decrypt the encrypted data portion*** only if access privilege of the user is successfully measured by the access rules," and Applicants could not identify how the information encrypting method of Sprague et al. and providing a "device" for decrypting is equivalent to providing a user key "***to access the access rules in the security information***," whereby "***the file key can be retrieved to access the encrypted data portion***."

Moreover, even if, *arguendo*, Sprague et al. does teach "activating a user key after the user is authenticated, wherein the user key is used to access the access rules in the security information, the file key can be retrieved to decrypt the encrypted data portion only if access privilege of the user is successfully measured by the access rules," Applicants assert that one of ordinary skill in the art at the time the invention was made would not have been motivated to combine Leporini et al. with Sprague et al. The

Examiner states that the motivation to combine the references is that the modification "would have ensured the information transmitted, received and/or stored by the system remains secure against unauthorized use and unlawful access."

However, Applicants fail to see where one of ordinary skill in the art at the time the invention was made would have been motivated to look to Sprague et al., or any other reference, to secure information against unauthorized use and unlawful access when Leporini et al. already encrypts the content management information and the conditional access information for security purposes and proposes that the "content management information may be encrypted using a different exploitation key from that used to encrypt the conditional access information, and may be encrypted using a different encryption algorithm" for still greater security (paragraph [0024]).

Based at least upon the above remarks, Applicants submit that claim 1 is allowable in view of the combination of Leporini et al. and Sprague et al. and request that claim 1 be allowed. Furthermore, since claims 2-15, and 17-19 depend from claim 1, Applicants submit that claim 2-15, and 17-19 are also allowable in view of Leporini et al. and Sprague et al. for at least the same reasons given above in conjunction with claim 1, and request that claims 2-15, and 17-19 also be allowed.

Regarding independent claim 20, the Examiner alleges in the Office action that Leporini et al. teaches "a method for providing access control management to electronic data in a client machine, the method comprising authenticating a user attempting to access the electronic data; maintaining a private key and a public key, both associated with the user, wherein the electronic data, when secured, includes a header and an encrypted data portion, the header further includes security information controlling who, how, when and where the secured electronic data can be accessed and the encrypted data portion is an encrypted version of the electronic data according to a predetermined cipher scheme (see paragraphs 0003, 0004, 0008, 0015, 0024, 0027, 0036, 0041-0046, 005200203 [sic], 00437)."

The language of present claim 20 recites:

20. A method for providing access control management to electronic data in a client machine, the method comprising:

authenticating a user attempting to access the electronic data;

maintaining a private key and a public key, both associated with the user, wherein the electronic data, when secured, includes a header and an encrypted data portion, the header further includes security information controlling who, how, when or where the secured electronic data can be accessed and the encrypted data portion is an encrypted version of the electronic data according to a predetermined cipher scheme;

encrypting the security information with the public key in the client machine when the electronic data is to be written into a store; and

decrypting the security information with the private key in the client machine when the electronic data is to be accessed by an application.

Claim 20 requires "authenticating a user attempting to access the electronic data." While Leporini et al. teaches an "encryption key [] associated with a device, subscriber, commercial offer, or content" (paragraph [0037]), Leporini et al. does not specifically teach a process of authenticating a subscriber who is attempting to access the electronic data. And as noted above with respect to claim 1, even if the unique user key of Leporini et al. is viewed as an identifier that identifies the user, the user key is not used to authenticate the user.

Claim 20 next requires "maintaining a private key and a public key, both associated with the user, wherein the electronic data, when secured, includes a header and an encrypted data portion, the header further includes security information controlling who, how, when or where the secured electronic data can be accessed and the encrypted data portion is an encrypted version of the electronic data according to a predetermined cipher scheme." Leporini et al. does not teach both public and private keys associated with a user. Leporini et al. does provide general and local exploitation keys (paragraph [0240]), but these keys do not constitute public and private keys associated with the user.

Even if, *arguendo*, the general and local exploitation keys are public and private keys associated with a user, claim 20 requires that both the encryption and decryption are performed in a client machine. The Examiner notes that Leporini et al. fails to teach encrypting the security information with the public key in the client machine when the electronic data is to be written into a store, and decrypting the security information with the private key in the client machine when the electronic data is to be accessed by an application. The Examiner alleges that Sprague et al. teaches these limitations and that

the motivation to combine the references is that the modification "would have ensured the information transmitted, received and/or stored by the system remains secure against unauthorized use and unlawful access."

Sprague et al., however, does not teach that both the encryption and decryption are performed in a client machine. For example, in the news service embodiment of Sprague et al., "[t]he data stream is [] encrypted before being transmitted to communications satellites 16" (col. 9 lines 30-32) and the customer terminal 30 decodes the transmitted data stream" (col. 9 lines 44-48). Thus, the encryption is not performed by the client machine.

In the other embodiment taught by Sprague et al., "[i]n this case the protected archival information is stored on high density media" (col. 16 lines 41-42). In other words, the protected archival information is distributed already recorded on the high density media, or is provided by broadcast in the encrypted state to be stored on the media (see FIG. 7). There is no indication that the IP is received by the user apparatus in an unencrypted state, only to be then encrypted and stored on the high density media; doing so would run counter to the object of "distributing information to a user which is extremely secure from attack and tampering by a third party and/or the user him/herself" (col. 3 lines 26-29). Thus, in this embodiment, only the decryption is performed by the client machine.

Moreover, one of ordinary skill in the art at the time the invention was made would not have been motivated to combine Leporini et al. with Sprague et al. for the reasons provided above with respect to claim 1.

Based at least upon the above remarks, Applicants submit that claim 20 is allowable in view of the combination of Leporini et al. with Sprague et al., and request that claim 20 be allowed. Furthermore, since claims 21-30 depend from claim 20, Applicants submit that claim 21-30 are also allowable in view of the combination of Leporini et al. and Sprague et al., viewed alone or in combination, for at least the same reasons given above in conjunction with claim 20, and request that claims 21-30 be allowed.

Regarding independent claim 31, the Examiner alleges in the Office action that Leporini et al. teaches "a method for providing access control management to electronic data, the method comprising receiving a request to access the electronic data; determining security nature of the electronic data; when the security nature indicates that the electronic data is secured, the electronic data including a header and an encrypted data portion, the header including security information controlling restrictive access to the encrypted data portion and the encrypted data portion is an encrypted version of the electronic data according to a predetermined cipher scheme (see paragraphs 0003, 0004, 0008, 0015, 0024, 0027, 0036, 0041-0046, 005200203 [sic], 00437)." Applicants note that here, too, this does not reflect the current state of claim 31 as provided in the listing of claims, above.

The language of present claim 31 recites:

31. A method for providing access control management to electronic data, the method comprising:

receiving a request to access the electronic data in a store;

determining security nature of the electronic data by intercepting the electronic data moving from the store through an operating system layer to an application for the data;

when the security nature indicates that the electronic data is secured, the electronic data including a header and an encrypted data portion, the header including security information controlling restrictive access to the encrypted data portion and the encrypted data portion including an encrypted version of the electronic data according to a predetermined cipher scheme,

determining from the security information if the user has necessary access privilege in the operating system layer to access the encrypted data portion without consulting with another machine; and

obtaining a file key and decrypting the encrypted data portion with the file key only after the user is determined to have the necessary access privilege to access the encrypted data portion, and thereafter the application receives the electronic data in clear form.

Claim 31 requires "determining [the] security nature of the electronic data by intercepting the electronic data moving from the store through an operating system layer to an application for the data." Leporini et al. teaches, with respect to playback of recorded programs with the HDVR, that "[a]t the time of using a recorded content, the CMPS ensures the validity of the associated rights by comparing the usage rules

presented in the recorded CMM with the rights acquired by the subscriber and included in the security module (SM)" (paragraph [0279]). Clearly, the security nature of the content of Leporini et al. is determined by comparing the usage rules presented in the recorded CMM with right acquired and included in the security module, rather than by intercepting the content itself. This is also made apparent by the examples of FIGs. 24-26. For example, with respect to FIG. 24, "[i]n stage 407, the SM decodes the CMMs, verifies that the time-shifting mode is authorized" (paragraph [0296]) then "[i]n stage 408, the HDVR module decrypts the control words, then sends them to the descrambler" (paragraph [0297]). Clearly, the security nature of the content is determined in stage 407 before the content is descrambled following sending the control words to the descrambler in stage 408. Therefore, the security nature cannot be determined by intercepting the content because the content is not sent until after the security nature is known.

Claim 31 also requires "determining from the security information if the user has necessary access privilege in the operating system layer to access the encrypted data portion without consulting with another machine." Again, Leporini et al. does not teach this limitation. For example, access privileges in Leporini et al. are handled in the Device Interface level 256. The Device Interface layer 256 is a different layer from the System Software/Hardware layer 258 which is the operating system provided by the manufacturer of the receiver/decoder (paragraph [0191]). The Device Interface layer 256 includes devices such as card readers (paragraph [0190]). Examples of low level devices 4068 are LCARD and RCARD devices which enable communications with smartcards in smartcard readers 4036 (paragraph [0194]). As noted above, the CMPS is distributed across security modules (SM) on smartcards, for instance, the conditional access smartcard 48 is identified with the CAS SM in paragraph [0339]. Thus, security information is determined by security modules at the level of devices in the Device Interface layer 256 and not at the operating system layer as required by claim 31.

Based at least upon the above remarks, Applicants submit that claim 31 is allowable in view of the combination of Leporini et al. with Sprague et al., and request that claim 31 be allowed. Furthermore, since claims 32-40 depend from claim 31, Applicants submit that claim 32-40 are also allowable in view of the combination of

Leporini et al. and Sprague et al., viewed alone or in combination, for at least the same reasons given above in conjunction with claim 31, and request that claims 32-40 be allowed.

In paragraph 37 of the Office action, the Examiner rejected claims 6-9, 26, and 27 under 35 U.S.C. §103(a) as being unpatentable over the combination of Leporini et al. and Sprague et al. in further view of Ozog et al. Applicants traverse the rejection.

Claims 6-9 depend from claim 1 and claims 26 and 27 depend from claim 20. It has been shown, above, that claims 1 and 20 are allowable over Leporini et al. and Sprague et al. The addition of Ozog et al. does not cure the deficiencies of Leporini et al. and Sprague et al. In light of this, Applicants request that claims 6-9, 26, and 27 be allowed.

In paragraph 38 of the Office action, the Examiner rejected claims 41-88 under the same rational as claims 1-40. Based at least upon the above remarks with respect to claims 1-40, Applicants submit that claims 41-88 are also allowable in view of Leporini et al. and Sprague et al. with or without Ozog et al., and therefore request that claims 41-88 also be allowed.

CONCLUSION

Should the Examiner make the next Office action final, Applicants remind the Examiner that, per MPEP §706.07 "the final rejection ... *should include a rebuttal of any arguments raised in the applicant's reply.*" Simply declaring that the arguments of the Applicants are not pursuasive, without detailed elaboration, will not further the goal of developing clear issues for appeal.

In the alternative, the Examiner may instead find new grounds of rejection and issue another non-final Office action. Following the Appeal Brief the Examiner has twice found new grounds of rejection and declared the Applicants' arguments moot. 37 CFR §1.104(c) notes that "[i]n rejecting claims for want of novelty or for obviousness,

the examiner must cite the best references at his or her command." Also per MPEP §706.07, "[s]witching from one subject matter to another in the claims presented by applicant in successive amendments, **or from one set of references to another by the examiner in rejecting in successive actions claims of substantially the same subject matter**, will alike tend to defeat attaining the goal of reaching a clearly defined issue for an early termination, i.e., either an allowance of the application or a final rejection."

Accordingly, Applicants urge the Examiner to either allow the application or make the next Office action final with a detailed rebuttal of Applicants' arguments that would be sufficient for the Applicants to either assess the advisability of an appeal or narrow the claims in further prosecution.

Based on the foregoing remarks, Applicants believe that the rejections in the Office action of June 7, 2005 are fully overcome, and that the Application is in condition for allowance. If the Examiner has questions regarding the case, the Examiner is invited to contact Applicants' undersigned representative at the number given below.

Respectfully submitted,
Alain Rossmann, et al.

Date: 9/6/05 By: Susan Yee

Susan Yee, Reg. No. 41,388
Carr & Ferrell LLP
2200 Geng Road
Palo Alto, CA 94303
Phone: (650) 812-3400
Fax: (650) 812-3444